44

This Copy No. 4 taken from Friedman File A 19-2/15 Brownell Committee, which contains Copies 1, 2, and comeback.

Korea

~~SECURITY INFORMATION~~

~~TOP SECRET GUEDE~~

~~TOP SECRET GUEDE - SECURITY INFORMATION~~

Copy No. 4

REPORT ON

SIMILARITIES AND DIFFERENCES BETWEEN [redacted] AFSA

IN REGARD TO ORGANIZATION, METHODS, AND ARRANGEMENTS

FOR

PROCESSING PLAIN-TEXT TRAFFIC FOR THE PRODUCTION OF COMINT

AND A FEW COMMENTS THEREON

By: WILLIAM F. FRIEDMAN

Date: 31 March 1952

~~TOP SECRET GUEDE~~

1. a. The term Communications Intelligence (COMINT) designates the information and technical material resulting from the interception and study of intercepted communications.[1]

b. The term traffic analysis (T/A) designates the operations involved in the study of the "externals" and characteristics of intercepted communications (procedure signals, message headings, call signs, etc., D/F bearings, Radio Finger Printing data, and other technical aids) for the purpose of obtaining information[2] concerning the organization and operation of the communication system or networks on which the communications are passing.

c. The term traffic intelligence (T/I) is that COMINT which is produced by drawing inferences or deductions from the information obtained by T/A operations defined above.

d. The term plain text (P/T) includes communications of two sorts:

(1) Category 1 - Plain-language communications passed on internal radio links of the country involved.

(2) Category 2 - Plain-language and [redacted] of the world.[3]

e. The term processing refers to the steps and operations performed on intercepted communications, up to and including their translation. It does not include the preparation of reports, appreciations, digests, etc., based upon the information constituting the end-product of the COMINT, T/A and T/I operations; that is, the term does not include the preparation of so-called finished "intelligence."

2. a. The principal differences between [redacted] AFSA organizations and arrangements for the processing of plain-text are as follows:

(1) [redacted] is currently organized on a centralized functional basis, that is, the structure as a whole

---

1. This and the following definitions apply to the terms as specifically used in this report.

2. This information is used (1) as a guide to efficient intercept control and operation, (2) as an aid to cryptanalysis, and (3) as a basis for what is defined in 1c.

3. [redacted] is included in this category because such codes are available and are intended for economy, not secrecy.

comprises nine large Departments which perform technically different operations. Thus, [redacted] so on. Within these Departments, and where desirable or necessary, the technical operations are organized on a geographical basis; for example, [redacted] also performs certain processing functions and these are the ones of immediate interest, since they include the processing of plain-text communications. [redacted]

(2) In the case of the AFSA COMINT establishment, the primary components of the organizational structure are separated on a functional basis but from there on down the separation is on a geographic-area basis. Referring to Appendix 2, it will be noted that the AFSA COMINT organization is divided up into three main Departments: Collection (O2-C), Processing (O2-D), and Evaluation (O2-E); under the Processing Department there are three divisions, the Machine Division (AFSA-22), the General Processing Division (AFSA-23), and the Special Processing Division (AFSA-24). Only the latter two are of concern in connection with this report. AFSA-24 deals only with [redacted] communications, except for certain T/A and other operations conducted in AFSA-242 on [redacted] plain-text; the detailed processing of [redacted] plain-text communications is conducted within AFSA-26, a separate division under the Chief of Evaluation (AFSA-02E), a matter which will be discussed detail presently. AFSA-23 deals with both encrypted and plain-language communications of all other governments; AFSA-23 is then subdivided on a geographic-area basis, somewhat like [redacted]

[redacted]

~~TOP SECRET SUEDE~~

[redacted] However, there is very close liaison between the workers in these geographical divisions and those in the homologous geographical divisions of [redacted]

(c) The organizational structure of the [redacted] indicating the position of the plain-text and other processing divisions, is shown in diagrammatic form in Appendix 3; the [redacted]

(4) (a) At AFSA, plain-text processing is conducted on a decentralized basis. The major part of the processing of [redacted] plain-language communications passed on all [redacted] internal links (Category 1), and [redacted] is done under one division[4] (AFSA-26) in the Office of Operations (AFSA-02).

EO 3.3(h)(2)
PL 86-36/50 USC 3605

(b) However, some processing (principally T/A and T/I) of internal [redacted] plain-text (Category 1) is done within several sections[5] of a branch (242) of the Special Processing Division (AFSA-24) under the Chief of Processing (AFSA-02D).

(c) Processing of [redacted] Category 1 and Category 2 communications is done within three geographical branches (B, C, D) of the General Processing Division (AFSA-23) under the Chief

---

4. The division "is responsible for the study and evaluation of Task I [redacted] plain-text traffic, and for the production of specialized intelligence information concerning Task I [redacted] economic and industrial organizations and capabilities, and studies on armed forces (Rear Area) as directed."

5. For example, AFSA-2420 works in close collaboration with other sections of AFSA-24 and with AFSA-26. Of important interest is the [redacted] this information being of direct use to the Plant Engineering personnel of AFSA-282. Among other duties this section prepares general plans, requirements, and equipment specifications for facilities of fixed intercept stations under operational control of AFSA. See Appendix 4 for the other sections of AFSA-242.

of Processing (AFSA-02D). Such T/A and T/I work as is necessary or can be done on these communications is also done within these same branches. These branches (AFSA-23B, C, D) also process encrypted communications and, in fact, the processing of both encrypted and plain-text communications is conducted as an integrated operation - the persons who do the cryptanalysis, T/A, and T/I on encrypted messages also process Category 1 and Category 2 plain-text messages in the various [redacted] languages involved.

(d) The organization of the Office of Operations in regard to the processing of plain text is also shown in diagrammatic form in Appendix 4.

[redacted] At AFSA there is now no counterpart to this, that is, there is no central unit for "reporting." In fact, such activities are supposed to be "illegal" so far as AFSA doing them is concerned.

(6) However, very recently a new departure has been made: certain units of AFSA-02 are preparing and issuing "reports," with the cognizance of the consumer agencies. Of special interest in this connection are the reports prepared in AFSA-23D, which deals with the Asiatic Area. These reports are of use principally to the Services, since they contain COMINT applicable to Communist [redacted] A similar but smaller reporting operation is conducted in AFSA-23C, the product of which is of special interest to CIA. If this sort of "reporting" were extended within AFSA-02, and especially if the "reports" prepared within

[redacted]

7. Army G-2 has several representatives working with AFSA-23D personnel in the preparation of these reports.

the various units were then passed to a central reporting unit for the whole of AFSA-02 as directed, I am of the opinion that not only would the efficiency of AFSA-02 operations be increased to an important degree but also the quality of the end-product considerably improved. Such a central reporting unit would be very advisable since it not only could fuse or integrate the reports prepared by various small reporting units in the processing sections and branches, but it could serve the important function of standardising terminology, format, etc. It is important to emphasize this phase in the differences between [redacted] AFSA mechanics in handling the P/L problem. [redacted] on subjects of interest to its consumers. The full-message translation method has been reserved for the very few items which can stand alone and tell a good story. Only in the case of special subjects [redacted] has there been any attempt to publish all available messages on a subject, and in these rare instances the translations are published in book form rather than as individual cards. On the other hand, AFSA has always been under some pressure to issue as large a number of individual translations as possible. The right to write reports is not universally now acknowledged. In the case of Shipbuilding, AFSA was enjoined to restrict its efforts entirely to message translation.

b. There is one area of the P/L picture which presents additional operational differences between [redacted] AFSA, namely those in connection with the handling of what is called "Foreign Trade Communications." Because of their very nature, foreign trade communications pass across the geographical boundaries established within both AFSA [redacted] operating divisions and branches, and unless the communications of both parties to an international trade activity or operation are available for study by one rather than two groups of COMINT workers, much can be lost in the way of intelligence. For example, messages involving foreign-trade deals may pass between Brazil and Czechoslovakia; if the study of such messages is divided on a geographic-area basis, one study group would handle only those originating in Czechoslovakia, although both sets of messages would be applicable to the same foreign-trade deal. Recognizing this fact, [redacted] In AFSA, however, the foreign-trade problem is split up among various branches of AFSA-23 and between AFSA-23 and AFSA-26. Such a split is clearly inadvisable and in my opinion it would be well for AFSA to follow [redacted] pattern in this area of the P/L problem and set up a single unit to process all foreign-trade communications of Category 2 type. In this respect, you will be interested to know that AFSA-02 has planned the same type of operation, the only problem delaying action being the shortage of critical linguists to work both plain language and cryptanalytic problems. The change may well be effected within the next 30 days.

c. A minor element of difference between [redacted] AFSA mechanics in handling the P/L problem is that involved in the scanning process. In [redacted] Here sorters are supplied with certain key words and catch phrases, so to speak. They are not linguists, but they do the first step satisfactorily because they are quite competent to sort according to only about six categories. The traffic, thus sorted into categories and links, is sent to [redacted] In the AFSA operation, there is no preliminary scanning at the intercept station and all the traffic is sent to AFSA, where a branch (AFSA-213) of the Traffic Division (AFSA-21) under the Chief of Collection (AFSA-02C) does the preliminary scanning such as is done at the intercept site in the case [redacted] the material is then sent to AFSA-26 where final scanning is done. (For the position of AFSA-213 in the organizational structure, see Appendix 4.)

3. a. It has been suggested in certain quarters (1) that [redacted] system of centralized P/L processing is more efficient and better than our own decentralized system, (2) that therefore we would do well to follow the [redacted] (3) that if so centralized the whole P/L processing operation could and should be lifted out of AFSA and made a responsibility of some other intelligence organization which might be more efficient in COMINT production from this source, and (4) that if not lifted out from AFSA working quarters the other intelligence organization should be permitted to conduct the integrated P/L processing by its own personnel in AFSA working quarters.

b. As to the first of the foregoing suggestions, I think it valid to say that if the [redacted] is more efficient (and I daresay it is) this is not because of but despite the centralization. Careful analysis of the technical picture leads me to the conviction that the primary factor which makes it more efficient is the fact that [redacted] not only permitted to engage in a so-called "intelligence function" but is encouraged and supported in doing so. [redacted] Instead of having to do what AFSA does, viz., process and translate millions of messages merely to turn them over to a duly authorized "intelligence-producing agency" which deems its prerogative to be to put the "bits and pieces" together to make an "intelligence story," [redacted] personnel are permitted to select, discard, summarize, extract, etc., from the original bits and pieces, this resulting in a much more efficient operation, since a "reporting" system eliminates the necessity of fully processing and translating large numbers of messages which may not be useful.[8]

8. An exception which is logical under a "reporting" system is in the case of decrypts of diplomatic messages. Here our State Department desires the verbatim texts, and rightly so. In fact, it would be well if those decrypts were turned over in their original languages in those cases where the foreign languages, [redacted] would present little difficulty for consumer-readers in the State Department. Incidentally, if this were done in the case of [redacted] a great deal of labor in AFSA would be saved by eliminating the need for translation. This practice is followed [redacted]

~~TOP SECRET SUEDE~~

In addition the end-product is probably of better quality, since small bits of information that turn up in processing are likely to be unknown to purely "intelligence" producing personnel who are merely recipients of translations. It is familiarity with all the bits and pieces that makes for better quality of the end product.

c. As to the second suggestion, I feel sure that regardless of which type of P/L processing is preferable (centralized or decentralized) the contact between the personnel processing P/L and those processing encrypted messages (including the T/A and T/I phases) must be exceptionally close. It is true that it is close [redacted] but in AFSA, in the case of three large geographical branches (AFSA-23B, C, D) which handle Category 2 traffic, it is not a case of close contact; the same people work on both encrypted and P/L traffic. It is logical that the processing activities be arranged so that this will be possible, for it is very often the case that whether a message will be sent in encrypted or in plain-language form is a decision of the originator and thus subject to his whim of the moment perhaps. Hence, it is occasionally found that both types of messages are sent on the same subject and therefore the plain-language ones form excellent "cribs" into the encrypted ones; on the other hand, the decrypted messages often make the plain-language ones more intelligible. In this connection, in Appendices 5 and 6 will be found additional technical reasons and examples why the same unit should handle both types of messages and why the AFSA system in this regard is, in my opinion, better than [redacted] system.[9] In short, centralization offers advantages, but so does decentralization, and the technical advantages of each in the specific case under discussion must be the guide as to how much of each type of working should be employed in any organization. I am told, in this connection by a recent AFSA visitor to [redacted]. have, as described above under paragraph 2a(1).

d. As to the third suggestion, I think I have said enough in the foregoing comments to indicate my conviction that while of course almost anything is possible and that the P/L processing could be put in one package and lifted out of AFSA, to do so would be a bad mistake. It would reduce efficiency in the processing of both P/L and encrypted communications.

---

9. Until recently internal [redacted] (Category 1) P/L traffic was processed by a section of a branch of the Special Processing Division (AFSA-24G); it is now processed by a separate division (AFSA-26) under the Chief of Exploitation (AFSA-02E); but even the close contact between the personnel working on internal [redacted] and those working on internal [redacted] P/L traffic cannot be as efficient as would be the case if the processing of both types of traffic were under the same division.

~~TOP SECRET SUEDE~~

e. Finally, as to the fourth suggestion, it is hardly necessary to point out the administrative and other problems of having personnel who do not belong to you work in your quarters but not under your administrative or operational control. There are enough cases of this sort of thing already - where the necessity for them is much more evident than in the case under consideration.

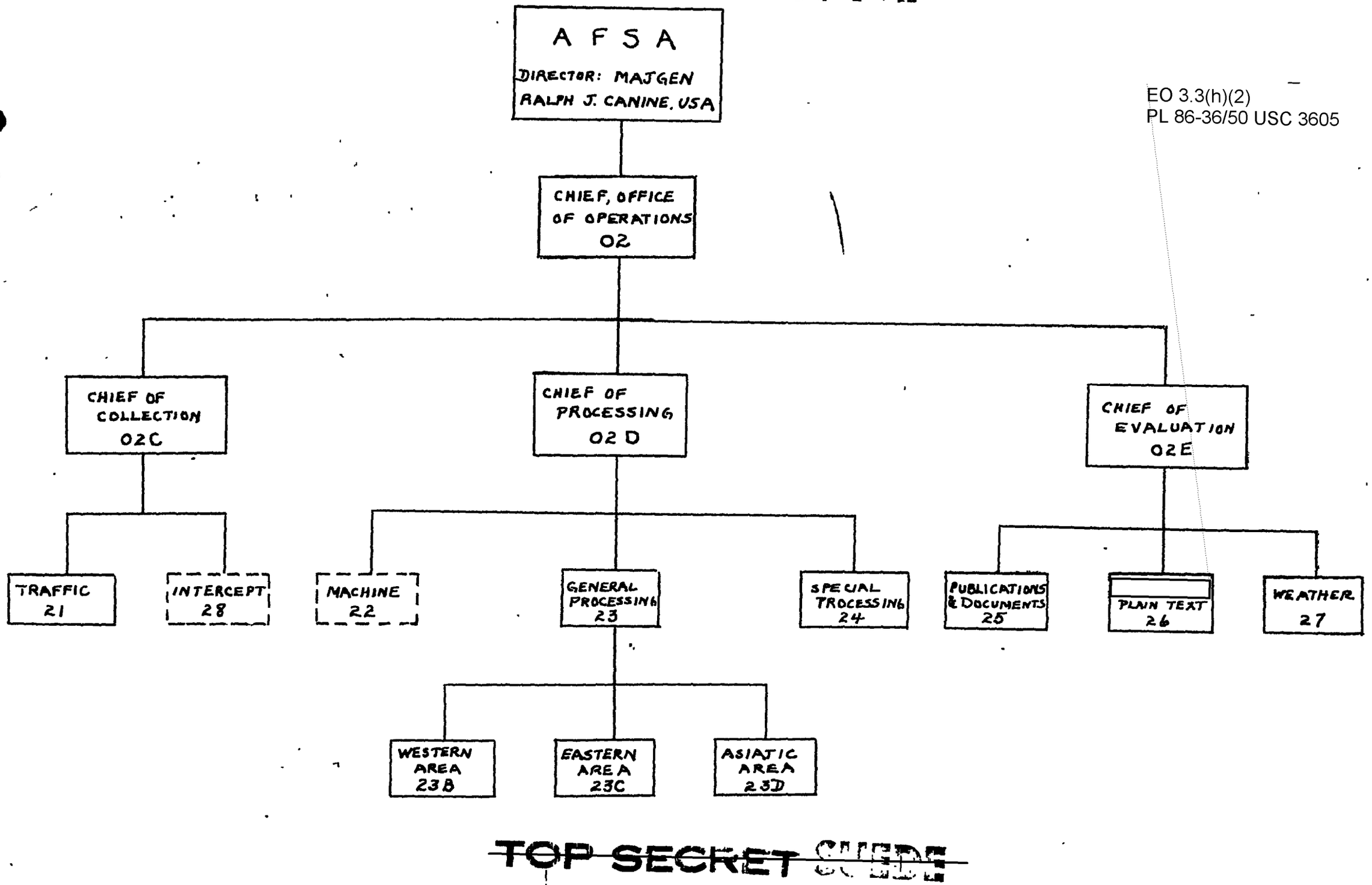
WILLIAM F. FRIEDMAN
Consultant

FUNCTIONAL ORGANISATION

1st JULY 1951

G.O.I. 2
EXHIBIT A

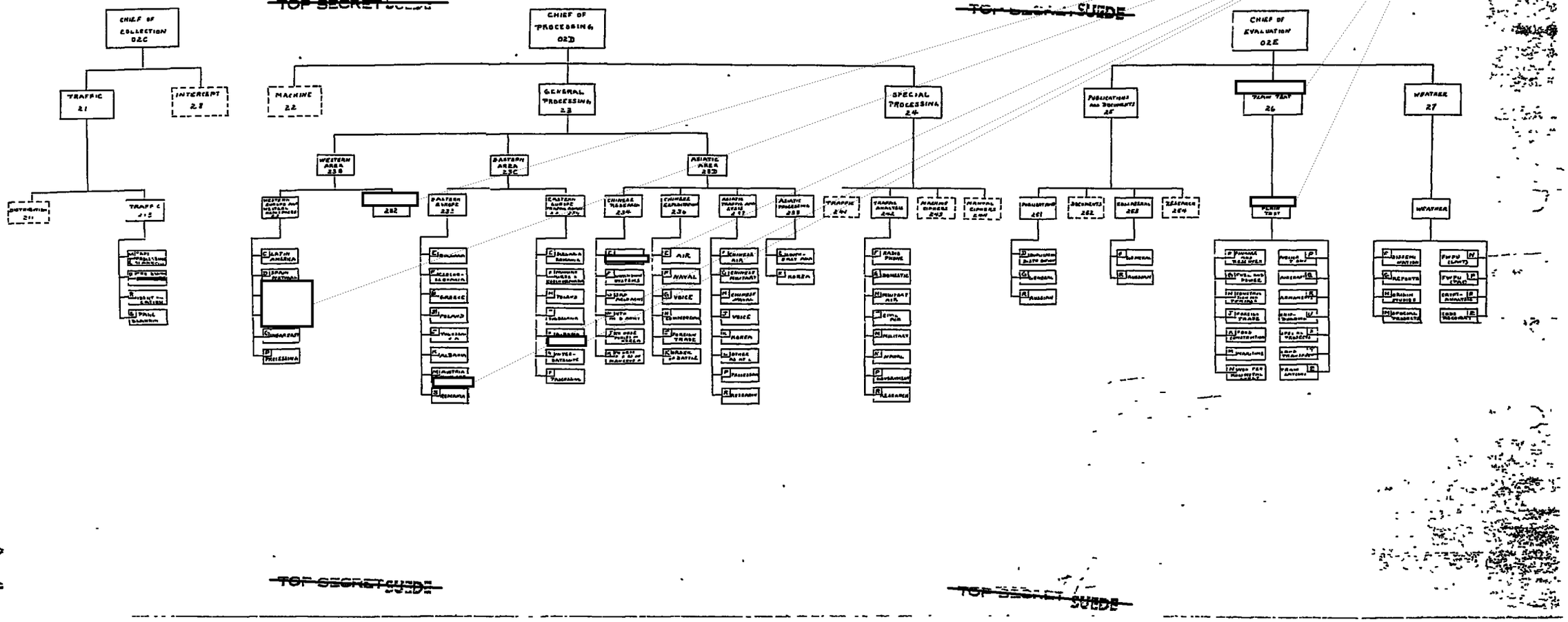
TOP SECRET CRYPTO



APP 2

TOP SECRET CRYPTO

App. 3



App 4